PERANCANGAN SISTEM PENCEGAHAN FLOODING DATA PADA JARINGAN KOMPUTER

MAKALAH

Disusun sebagai salah satu syarat menyelesaikan Jenjang Strata I

pada Program Studi Informatika Fakultas Komunikasi & Informatika

Universitas Muhammadiyah Surakarta

Oleh :

Ridlwan Pahala

NIM : L200090151

PROGRAM STUDI INFORMATIKA

FAKULTAS KOMUNIKASI DAN INFORMATIKA

UNIVERSITAS MUHAMMADIYAH SURAKARTA

JULI 2015

HALAMAN PENGESAHAN

Publikasi ilmiah dengan judul :

PERANCANGAN SISITEM PENCEGAHAN FLOODING DATA PADA JARINGAN KOMPUTER

Yang dipersiapkan dan disusun oleh :

RIDLWAN PAHALA

NIM : L200090151

Hari : Sabtu

Tanggal : 11 Juli 2015

Pembimbing

Muhammad Kusban, S.T.,M.T.

Publikasi ini sebagai salah satu persyaratan

Untuk memperoleh gelar sarjana

Tanggal : 12 Desember 2015

PERANCANGAN SISITEM PENCEGAHAN FLOODING DATA PADA JARINGAN KOMPUTER

RIDLWAN PAHALA
Informatika, Fakultas Komunikasi dan Informatika
Universitas Muhammadiyah Surakarta
E-mail : ridwanscumbag@gmail.com

ABSTRAKSI

Suatu serangan ke dalam *server* pada jaringan komputer dapat terjadi kapan saja, baik pada saat *administrator* sedang bekerja maupun tidak. Dengan demikian dibutuhkah suatu keamanan pada server itu sendiri yang mampu mendeteksi secara langsung apakah setiap paket data tersebut merupakan paket data yang sebenarnya atau tidak. Apa bila paket tersebut merupakan paket yang dikirim oleh penyerang,maka sistem secara langsung akan memblokir IP dari pengirim data tersebut. Flooding data yang terjadi hanya bisa dicegah dari server saja, dan hanya bisa mencegah data yang masuk kedalam jaringan yang mungkin dapat menimbulkan kerusakan yang lebih parah.

Deteksi atau pencegahan ini dilakukan untuk mengetahui adanya flooding data pada suatu jaringan komputer. Deteksi dan pencegahan ini dilakukan dengan sistem yang didesain dengan membangun *firewall* aktif yang dapat mendefinisikan setiap data yang masuk kedalam *server* merupakan data yang dibutuhkan user atau merupakan data flood.

Kata kunci : keamanan jaringan komputer,flooding data,firewall

PENDAHULUAN

Perkembangan teknologi yang demikian pesat akhir-akhir ini membutuhkan antisipasi yang cepat, tepat dan akurat dalam penyelesaian semua permasalahan yang muncul. Kecepatan penanganan, ketepapan menanganalisa permasalahan, lalu mengambil tindakan secara akurat akan menjadikan permasalahan yang muncul akan cepat teratasi.

Hal yang serupa juga terjadi pada dunia computer khususnya pada suatu system dimana satu kamputer terhubungan dengan computer lain untuk saling berbagai data dan informasi yang mereka miliki. Kemudahan akses untuk mendapatkan data antar computer dan bertukar informasi satu dengan lain menjadikan computer bagian hidup yang sangat penting.

Dalam suatu system yang luas, diperlukan suatu sentral atau pusat system sebagai pengawas lalu lintas data. Pusat system tersebut dinamakan sebagai server. Dalam lalu lintas data yang demikian cepat, keberadaan server sangat penting selain sebagai pengatur data yang keluar masuk, memisah data mana yang masuk terlebih dahulu dan mana yang keluar terlebih dahulu dan juga sebagai pengatur siapa dan data apa yang dapat diambil oleh pengguna.

Kemajuan teknologi juga menjadi pisau bermata dua yang pada satu sisi menguntungkan dan pada sisi lainnya memberikan kerugian. Berkaitan dengan lalu lintas data dalam suatu jaringan computer, banyaknya data yang keluar masuk akan menimbulkan banjir data (flooding data) yang jika tidak dikendalikan dengan baik, bukan memberikan keuntungan terhadap pengguna namun akan menimbulkan kerugian. Flooding data tersebut antara dapat disebabkan oleh pertukuran data yang memang sangat padat atau disebabkan karena ada pihak-pihak tertentu dengan tujuan tersendiri yang sengaja mengirim dan mengambil data secara terus menerus pada server yang sama sehingga pada akhirnya menimbulkan permasalahan pada system yang bekerja tersebut. Berdasarkan hal tersebut maka peneliti mengangkat judul Perancangan Sistem Pencegahan Flooding Data Pada Jaringan Komputer

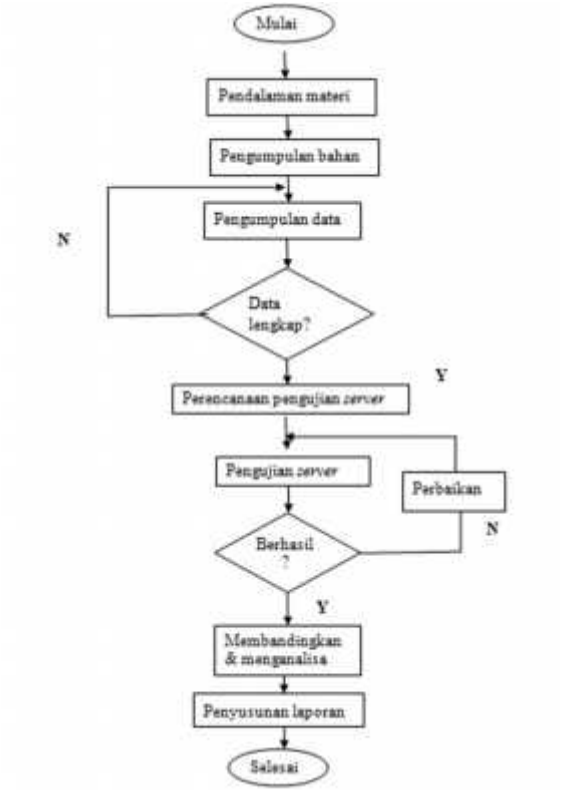
METODE PENELITIAN

Perancangan aplikasi perancangan sistem pencegahan flooding data ini bertujuan untuk memberikan pengetahuan tentang adanya sebuah serangan flooding data pada jaringan kompuer,sehingga para pengguna jaringan komputer dapat memonitoring traffic data mereka.

Alur penelitian

1. Diagram Alir *(Flowchart)* Penelitian

   Proses penelitian pembuatan aplikasi sistem flooding data pada jaringan komputer ini dimulai dari analisis pengumpulan bahan sampai dengan laporan, adapun proses/tahapan penelitian digambarkan dalam sebuah *flowchart* seperti pada Gambar 1 :



Gambar 1 Diagram Alir

Keterangan Diagram Alir :

Mulai : memulai proses pembuatan penelitian sesuai jadwal kegiatan yang telah ditentukan.

Pendalaman materi : melakukan pembelajaran dan memahami materi – materi yang akan digunakan dan dibutuhkan dalam pengerjaan penelitian.

Pengumpulan bahan : melakukan pengumpulan peralatan dan bahan – bahan yang akan digunakan dalam penelitian.

Pengumpulan data : pengumpulan referensi, Jurnal, Tutorial, dan data –data yang berhubungan dengan judul penelitian.

Data lengkap : melakukan pengecekkan kelengkapan data – data jika mengalami kekurangan maka akan kembali ke proses pengumpulan data, jika data lengkap akan dilanjutkan ke proses selanjutnya.

Membandingkan & menganalisa : setelah melakukan pengujian maka akan dimulai melakukan proses perbandingan dan analisa terhadap data – data yang telah didapat.

Penyusunan laporan : memulai penulisan pdan pembuatan laporan penelitian sesuai dengan data – data yang telah diperoleh darai pengujian.

Selesai : penelitian telah selesai.

Pengujian sistem

Untuk melakukan pengujian tersebut tersebut penulis melakukan hal hal berikut

1. Menjalankan sebuah prototype dari sebuah hubungan host-to-host
2. Melakukan konfigurasi pada sistem
3. Melakukan monitoring pada prototype LAN tersebut
4. Melakukan flooding ke host yang telah diberi sistem
5. Melihat hasil dari sistem apakah data flood dapat di blok atau tidak

Program Penguji

Untuk mengetahui program jalan atau tidak tentunya harus disimulasikan suatu kejadian yang mencerminkan keadaan yang sebenarnya. Untuk mendapatkan suatu flood yang disebabkan protokol dalam keadaan sebenarnya adalah susah dan jarang terjadi, sehingga dibuat suatu program yang digunakan mengirimkan paket-paket data melalui protokol TCP, UDP dan ICMP.

Pada program ini akan mengirimkan paket-paket secara kontinyu dan ukuran yang beraneka ragam sesuai yang diinginkan. Port yang digunakan juga bisa di tentukan sebelumnya, sehingga dapat menyerupai flood yang sebenarnya.

Berikut ini gambar dari program flood yang dipakai

Gambar 2 penguji flood

Keterangan gambar :

1. **Host**, merupakan bagian yang menunjukkan kemana data akan dikirim. Dalam kejadian flood host adalah korban yang akan di flooding.
2. **ICMP**, merupakan pengiriman paket ICMP. Yang perlu diatur dalam hal ini adalah :

a. **Freq** , selang pengiriman setiap paketnya. Satuan yang diatur adalah milidetik

b. **Length,** besar setiap yang dikirimkan.

3. **UDP**, merupakan pengiriman paket UDP. Yang perlu diatur dalam hal ini adalah :

a. **Freq** , selang pengiriman setiap paketnya. Satuan yang diatur adalah milidetik

b. **Length,** besar setiap yang dikirimkan

c. **Port,** port yang akan digunakan untuk mengirimkan data tersebut

4. **TCP**, untuk paket TCP tidak bisa dikirimkan secara langsung tapi dibutuhkan suatu Trojan untuk mengaktikan pengiriman paket dan membuka port yang akan dilalui sehingga paket TCP SYN bisa di kirimkan secara kontinyu.

Gambar 3 aplikasi trojan

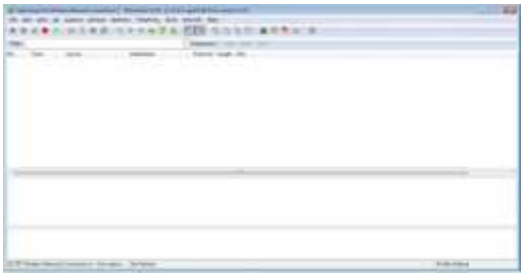
Keterangan Gambar :

Host : menentukan IP yang akan diserang memnggunakan aplikasi trojan tersebut

Freq : menentukan frequensi waktu penentuan jarak serangan terhadap Host yang akan diserang.

Port : menentukan port yang akan diberi flooding mengggunakan aplikasi trojan

HASIL DAN PENGUJIAN



Gambar 4 monitoring program

Program yang digunakan untuk monitoring adalah wireshark,dikarenakan program tersebut mempermudah untuk melakukan monitoring jaringan

Option program

Sistem melalui option yang ada untuk mengatur apa saja yang merupakan batasan dari sistem. Option program yang harus diisikan untuk memudahkan pengaturan program.

Bagian-bagian dari option program adalah:

Gambar 5 Option program

1. **Option ICMP**

   Merupakan bagian untuk menentukan sensitifitas flood detektor, yang akan digunakan pada pendeteksian ICMP flood. Bagian ini terdiri dari dua bagian yaitu :

   a. panjang atau ukuran maksimal dari paket yang datang. Apabila paket ICMP yang datang melebihi standar dianggap sebagai tindakan atau usaha flooding, sehingga paket tersebut perlu di teliti lebih lanjut untuk memastikan apakah paket yang datang tersebut adalah flood.

   b. Banyaknya paket maksimal setiap 10 detiknya. Banyak nya paket ini akan menentukan apakah data tersebut flooding atau tidak. Jika data yang datang banyaknya setiap 10 detiknya melebihi ketentuan akan juga diidentifikasikan sebagai usaha untuk flooding. Option ini berguna untuk mendeteksi data dengan paket besar.

   c. Banyak paket maksimal setiap detiknya. Untuk mendeteksi paket yang dikirimkan adalah paket kecil. Apabila ada paket kecil yang datang lebih dari

ketentuan setiap detiknya maka dianngap merupakan paket flood.

d. Apabila kedua syarat tersebut dipenuhi maka data-data ICMP yang datang tersebut dikatergorikan sebagai flooding.

2. Option UDP

Pada bagian ini hampir sama pengaturannya dengan ICMP, karena dianggap untuk sekarang data-data UDP belum dijadikan protokol transfer yang digunakan untuk pengiriman data yang besar. Pengiriman data yang mempunyai panjang paket terbesar hanya berlangsung di protokol TCP saja. Sehingga pada pengaturannya sama seperti paket ICMP yaitu:

a. Panjang maksimal dari paket UDP yang datang, apabila paket yang datang memiliki pangang lebih dari panjang maksimal dianggap sebagai usaha untuk melakukan flood yang perlu mendapat perhatian khusus.

b. Banyak nya paket yang diterima dalam 10 detiknya. Banyak paket UDP yang datang apabila banyaknya melibihi standar yang ditetapkan akan dianggap sebagai usaha dari pakte tersebut untuk melakukan flood. Digunakan untuk mendeteksi paket besar.

c. Banyak paket maksimal setiap detiknya. Untuk mendeteksi paket UDP yang dikirimkan adalah paket kecil. Apabila ada paket kecil yang datang lebih dari ketentuan setiap detiknya maka dianngap merupakan paket flood

Jadi apabila kedua syarat itu terpenuhi maka paket yang datang bisa dianggap flood.

3. Option TCP

Pada penerimaan paket TCP panjang tidak menjadi variabel dari paket untuk menunjukkan paket tersebut dianggap flood atau bukan, karena pada paket TCP kebanyakan memiliki panjang paket yang lebar. Sedangkan variabel yang dipakai apabila data terebut ingin melakukan flood atau tidak adalah:

a. Port yang digunakan. Port yang digunakan adalah port dari server yang sudah didefinisikan terlebih dahulu. Apabila ternyata paket TCP yang datang mengambil port yang tidak diperbolehkan dari server. Maka secara langsung paket tersebut dianggap melakukan flooding.

b. Lama perhitungan. Lama waktu yang ditentukan untuk melakukan satu kali identifikasi dari paket TCP SYN.
c. Banyak max paket TCP SYN, jumlah maksimal dari paket TCP SYN yang datang setiap waktu yang ditentukan. Apabila melebihi dari banyak yang ditetapkan sudah dipastikan paket-paket tersebut melakukan flood pada jaringan

HASIL PENGUJIAN

Pada proses pengujian ini, client yang bertindak sebagai penyerang mengirimkan paket-paket SYN ke dalam port-port yang sedang berada dalam keadaan terbuka yang berada dalam *server target*. Pada kondisi normal, paket-paket SYN yang dikirimkan berisi alamat sumber yang menunjukan data-data aktual. Tetapi pada serangan SYN Attack, paket-paket tersebut memiliki alamat sumber yang tidak menunjukan data aktual. Ketika server menerima paket SYN tersebut, server merespons dengan sebuah paket SYN/ACK sesuai dengan *SYN Packet* yang ia terima dan kemudian akan menunggu paket ACK sebagai balasan untuk melengkapi proses tersebut. Tetapi, karena alamat sumber dalam paket SYN yang dikirimkan oleh penyerang tidaklah valid, mak paket ACK tidak akan pernah terkirim ke target.

PEMBAHASAN

Yang di uji dari sistem adalah :

1. Kemampuan sistem untuk mengambil data.
2. Kemampuan sistem untuk mengklasifikasikan data-data yang ada
3. Kemampuan sistem untuk menyimpan data kedalam database
4. Kemampuan sistem untuk mendeteksi Flood.
5. Kemampuan sistem untuk melakukan blooking pada data yang terbukti Flood.

KESIMPULAN DAN SARAN

1. Sistem dapat mendetksi adanya floding data, sehingga semua dapat dilihat bahwa data tersebut merupakan data flood atau tidak. Data yang disebut flooding adalah data yang dikirimkan secara terus menerus dalam kurun waktu 10 detik dengan besaran data 100 Byte
2. System dapat bekerja meskipun diberikan flood yang besar karena

pembatasan paket data yang masuk merupakan variable yang bisa diubah besar kecilnya maka berapapun besar flood yang masuk dapat dideteksi. Hal ini seperti trlihat bahwa tidak semua data yang mempunyai ukuran sama.

3. System mampu mengatasi sendiri dengan pengambilan keputusan data masuk apakah flood atau bukan. Dan sekaligus melakukan tindakan akhir apabila terjaid flood yaitu dengan melakukan blooking data.

SARAN

Beberapa saran yang dapat peneliti sampikan dari hasil penelitian dan pembahasan yang telah dikemukakan diatas adalah sebagai berikut:

1. dalam melakukan pengawasan terhadap alira data yang masuk sebaiknya dilakukan pengamana berlapis dan adanya serifikasi terhadap data tersebut.
2. Sebaiknya dilakukan adanya batasan dalam melakukan pembatasan besarnya data yang dikirm dalam satu waktu tertentu, yang berguna juga untuk kelancaran jaringan pada system yang bersangkutan.

PERSANTUNAN

Makalah ini disusun agar dapat memenuhi salah satu syarat dalam mendapatkan gelar sarjana pada Program Studi Informatika Fakultas Komunikasi dan Informatika Universitas Muhammadiyah Surakarta. Terselesaikannya makalah ini tidak lepas dari dukungan dan bantuan dari pihak lain. Oleh karena itu dalam kesempatan ini penulis mengucapkan terimakasih kepada :

Dr. Heru Supriyono, M.Sc selaku Ketua Jurusan Teknik Informatika Universitas Muhammadiyah Surakarta dan Muhammad Kusban, S.T.,M.T. selaku pembimbing yang senantiasa memberikan waktu, nasehat dan bimbingannya kepada penulis sehingga dapat menyelesaikan makalah penelitian ini.

DAFTAR PUSTAKA

Syujak, Ahmad Rois 2012. *Deteksi Pencegahan Flooding Data pada Jaringan Komputer,* Skripsi, Universitas Muhammadiyah Surakarta, Surakarta.

Sarosa, M., dan Anggoro, S. Jaringan Komputer Data Link, Network dan Issue. Teknik Sistem Komputer Elektronik ITB. 2000.

Delphi Developers Information and ComponentsWilliam".2009-11-10. http://www.magsys.co.uk/delphi

http://ilmu27.blogspot.com/2012/08/makalah-keamanan-jaringan-network.html, diunduh pada Pkl.22.00 wib, 29 Mei 2013.

Fung, K. T. (Kwok T.). 2004. Network security technologies / Kwok T. Fung.--2nd ed, Boca Raton, Florida, USA. 2006.

Narvaez, L., Perez, J., Garcia, C., dan Chi, V. Designing WLANs for VoIP and Data. IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.7, July 2007

Brenton Ch., dan Hunt C., Network Security, alih bahasa : Hidayat J., PT Elex Media Komputindo, Jakarta, 2005.